Security technology

Security is a priority for our users and for us. We undertake to offer a platform that provides confidentiality, integrity, and security of your information. Our seed *sprint* ™ application is meant to deliver a safe environment for our customers to list and share information, dialogue and transact collaboration arrangements. The technologies used by seed *sprint* reflect our effort to deploy the appropriate and effective standards based on the current state of the art, and our business goal of keeping your data secure and available for seed *sprint* 's intended uses.

Key security features of our technology:

- All information is hosted in a resilient high-security data center in Staten Island, NY, operated by the Port Authority of New & Jew Jersey, Teleport. http://telehouse.com/pdf/Facilities_7TELEPORT.pdf
- To protect data, all transmissions to and from our server are protected by SSL with the highest encryption algorithm available today. This is similar to the algorithms used by major financial institutions. Symantec Secure Site with EV is our security certificate provider. If your web browsers supports the advanced security feature of displaying the green security bar, you can click on the bar to view more details about the certificate and the verification that you are on seedsprint.com.
- Confidential information, whether for a user's "Deep-dive package" or otherwise, immediately undergoes an encryption process, which may last a few milliseconds for small files, or possibly minutes, for very large files.
- Each file uploaded by a user is encrypted by our server and can only be decrypted using a key specific to that file.
- When a user authorizes another user to view and download files, after being unencrypted for the authorized request, the unencrypted file is deleted from the system so that only the encrypted file remains after the authorized access has been completed.
- We employ web security technology that actively scouts for threats and alerts us to possible threats.
- We certify all our applications and systems for effective security controls based on industry best practices

For more details on how we keep you and your information safe, please consult the FAQ:

1. **How is my identity protected on seed *sprint* ?**

We will not sell or rent your information to anyone. We share only your non-confidential information, and do so only with seed *sprint* subscribers. Our privacy policy describes how we protect your personal privacy and keep your personal information secure. For more information on our Privacy Policy please click here.

2. **How do you protect my account credentials (usernames/passwords) and information?**

The credentials you provide to us (usernames and passwords) are entered through Secure Socket Layer (SSL) encryption layers and we use encrypted user session technology as well. These technologies create and maintain an encrypted connection between your browser and our servers. Your credentials are stored in a encrypted format using SHA 512, a one way security protocol that is even stronger than AES, used by many banks. Your documents remain encrypted while they are on our server, and after they are made accessible to a user authorized by you, all unencrypted files are deleted so that only encrypted files remain post access.

3. **Where is my account information stored?**

Our platform is hosted and managed by Typhon Inc. on their dedicated servers, sited within an SAS 70 Type II certified center which is located in a designated high-level security zone with 24/7 security and biometric controls, operated by Teleport at their facility in Staten Island, NY. For more site and security information http://telehouse.com/pdf/Facilities_7TELEPORT.pdf

4. **Who has access to my seed *sprint* account?**

You create your seed *sprint* account password and you shouldn't give it to anyone else. No one can access your account unless you provide him or her with that information. If you forget your password, you must answer security questions before you can reset your password.

5. **How is my account information protected from loss or corruption?**

All information is backed up daily. The back ups are retained and rotated offsite. We regularly test our ability to restore our databases and files to protect you from data corruption.

6. **What can I do to protect myself and my personal information?**

You play an important part in securing your information and privacy. Some actions you can take:

- Review our "Web site account best practices"
- Keep computer and browser software current with security updates;
- Install and maintain current anti-virus and anti-spyware software; use personal firewalls to protect your computer;
- Change your password periodically and do not passwords you use for other accounts;
- Be aware of viruses, Trojans and all mal-ware (malicious software) that can hurt or disrupt your system or secretly record information like keystrokes;
- Consult the FTC computer security page, and Microsoft's and Apple's pages http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm , http://microsoft.com/security , and http://apple.com/support/security for more tips and recommendations;

Web Site Account Best Practices

When selecting your "Secret Question" choose answers that are not easily available to someone else. Example: If your Secret Question is "What was your pet's name?" that shouldn't be easy to find on the web, e.g., your Facebook page, etc., or you should use a different name that you can remember.

Tips for creating a secure password:

- Include symbols [/.!@# etc..]and/or numbers.
- Mix capital and lowercase letters.
- Include similar looking substitutions, such as the number zero for the letter 'O' or '$' for the letter 'S'.
- Create a unique acronym.

Things to avoid:

- Don't use a password that contains personal information (name, birth date, etc.)
- Don't use words or acronyms that can be found in a dictionary.
- Don't use keyboard patterns (asdf) or sequential numbers (1234).
- Don't make your password all numbers, uppercase letters or lowercase letters.
- Don't use repeating characters (aa11).

Tips for keeping your password secure:

- Don't tell your password to anyone.
- Never write your password down.
- Don't send your password by email.
- Change your password every two months.